NYU TANDON SCHOOL OF ENGINEERING

CS-6963 Digital Forensics - Spring 2021
Professor: Michael R. Berger, (MSc)^2
Teaching Assistants:N/A

COURSE OVERVIEW

This course introduces students to the application of forensic science principles and practices for collecting, examining, analyzing and presenting digital evidence. The course includes selected topics from the legal, forensic, and information technology domains and utilizes lectures, assignments and programming projects to illustrate these topics. We will explore these topics through the use of various open-source forensic tools.

PREREQUISITES

While there may not be prerequisites listed, students should have a knowledge level equivalent to an undergraduate or higher level course in Operating Systems, and an undergraduate or higher level course in Networking. Additionally, students should be comfortable scripting in Python and familiar with programming in C/C++.

LEARNING OBJECTIVES

By the end of this course students should be able to:

- Understand and describe how forensic science is applied to the cyber realm
- Identify and describe sources of digital evidence
- Develop custom scripts & programs to perform automated forensic analysis
- Understand file systems and their operational artifacts which both aid and hinder forensic analysis
- Conduct forensic analysis of both disk images and network data
- Acquire and analyze volatile memory
- Identify and describe basic legal principles regarding digital forensics
- Understand and perform basic static and dynamic malware analysis
- Describe how the concepts of digital forensics can be applied to aid in threat hunting
- Understand how digital evidence artifacts can aid in an intrusion investigation

COURSE STRUCTURE

This course is conducted entirely online, which means you do not have to be on campus to complete any portion of it. You will participate in the course using NYU Brightspace located at https://brightspace.nyu.edu.

GRADING BREAKDOWN

Forensic Analysis Assignments	40%
Programming Assignments	25%
Quizzes	20%
Technical Writing Assignment	15%

LEARNING TIME RUBRIC

Learning Time Element	Asynchronous* / Synchronous**	Time on Task for Students (weekly)	Notes
Lecture (Active Module)	(A)synchronous	1 - 2 hours	Live lecture via Zoom, also recorded for anyone who can not view at the scheduled time.
Active participation	Asynchronous	0.25 hours	Students discuss weekly lessons or topics related to the course
Reading	Asynchronous	1-2 hours	Students complete required readings for each module to help reinforce lecture content and prepare for the weekly quiz
Assignments	Asynchronous	4 -5 hours	Students independently work on assignments.
Quizzes	Asynchronous	1 hour	Students complete the weekly quiz

*Asynchronous learning is defined as any non-real time student learning, such as recorded lecture, podcast, interactive module, articles, websites, etc. This also includes any student-to-student or faculty-to-student communication that may happen with an asynchronous tool, such as discussion board, chatroom, e-mail, text, etc.

**Synchronous learning is defined as any real-time student-to-student and/or faculty-to-student learning, such as a live webinar session or other video/audio communication service.

WEEKLY MEETINGS - Tuesdays @ 8pm EST (subject to change)

We will meet each week via Zoom and go over the content listed on the syllabus. For anyone who can't attend live, each meeting will be recorded and posted shortly after, for everyone to view. There is no direct grade penalty for not attending live classes, although students should make an effort to attend live whenever possible. Notice will be sent via email if the day/time changes for a specific week.

READING MATERIAL

Students should expect reading material to be provided each week, to supplement the material presented in the lecture, usually in the form of journal articles and research papers. When provided, this material should be read and understood prior to taking the weekly quiz.

COURSE PACE

The course is structured so as to allow a constant pace of work throughout the semester, while allowing flexibility with most due dates for student's schedules. Some specific non-flexible due dates will be announced well in advance. Students who do not adhere to the recommended schedule of doing each module's work each week will quickly fall behind and struggle greatly towards the end of the semester.

ASSIGNMENTS

Students should anticipate weekly assignments in the class, with work generally being assigned Monday morning. To stay on pace, you should aim to complete each assignment by the following Sunday evening, prior to the next module beginning on Monday. These assignments will help to reinforce the concepts covered in the lectures and the readings, and help build your practical analysis skills.

FORENSIC ANALYSIS ASSIGNMENTS

These assignments will serve to help students learn practical digital forensic analysis techniques, and are thus one of the most important aspects of the overall class. Most assignments will be found under the "Quizzes" section of Brightspace, however there will be no set time limit for the assignment..

PROGRAMMING ASSIGNMENTS

These assignments will help you apply your programming skills to common challenges you will encounter performing digital forensic analysis which are best served by being able to write a custom script or tool. They will also help to further your understanding of what happens "under the hood" of standard forensic tools, in an effort to elevate your knowledge past the level of "pushing buttons in a tool". These assignments will be submitted via Gradescope for automated evaluation and feedback. Students will have unlimited submissions through the final course submission deadline in order to utilize the feedback provided to improve their submission.

QUIZZES

Students should expect a quiz each week, which will cover the content in the lecture, as well as the reading material assigned when applicable. You may take the quiz whenever you are ready, up until the final course submission deadline. The quiz is "open-book", however you should not take it until you have attended/watched the lecture and read the corresponding reading material, as you will not have enough time to look up every question. These are designed as more of a knowledge check, to ensure you are keeping up with the weekly content and understanding the material. Quizzes will generally be about 10 questions with a 20 minute time limit.

TECHNICAL WRITING ASSIGNMENT

This assignment involves reading the "The Cuckoo's Egg", and writing a comparative technical analysis of forensic techniques used in the book vs. what is currently available today. The book tells the true story of one of the first known instances of a foreign adversary based cyber intrusion, and the subsequent investigation undertaken by the victim entity. The assignment serves as an opportunity for students to develop their abilities to write about advanced technical analysis in order to inform the reader, as well as to analyze forensic analysis performed by someone else in order to evaluate the processes and techniques.

For this assignment, you will be submitting your paper to Brightspace and we will utilize the peer review functionality.. As an additional part of the assignment, once papers are submitted, you will be tasked with reading and providing feedback on three of your peer's assignments. This process allows the assignment to also help you develop skills pertaining to reviewing and providing feedback on technical documents. The feedback process will be anonymous on both sides (you will not know whose papers you are grading, and you will not know who provides the feedback to you), and I will be overseeing the process.

WEEKLY VIRTUAL OFFICE HOURS

The instructor will be available for weekly virtual office hours by appointment. To schedule an appointment, or to ask any questions about the course content, please email them.

ANNOUNCEMENTS

Announcements will be posted on Brightspace on a regular basis (and automatically emailed to you by default). You can locate all previous class announcements under the Announcements tab of our class. Be sure to check the class announcements regularly as they will contain important information about class assignments and other class matters.

EMAIL

You are encouraged to post your questions about the course in the Forums discussions on NYU Classes. This is an open forum in which you and your classmates are encouraged to answer each other's questions. But, if you need to contact me directly, please email me at mrberger@nyu.edu. You can usually expect a response within 24 hours.

COURSE MATERIALS

REQUIRED READING MATERIAL

Title: The Cuckoo's Egg:
Tracking A Spy Through The Maze Of Computer Espionage
Author: Cliff Stoll
ISBN: 1416507787

RECOMMENDED REFERENCE MATERIAL

Title: Digital Evidence and Computer Crime:
Forensic Science, Computers, and the Internet, 3rd Edition
Author: Eoghan Casey
Publisher: Academic Press
ISBN: 9780123742681

Title: The Art of Memory Forensics
Author: Michael Hale Ligh, Andrew Case, Jamie Levy, AAron Walters
Publisher: Wiley
ISBN: 1118825098

Title: File System Forensic Analysis (1st Ed.)
Author: Brian Carrier
Publisher: Addison-Wesley, 2005
ISBN: 0321268172

COURSE SCHEDULE

The following is the list of topics we will be covering, and the anticipated schedule for each, subject to change due to unforeseen circumstances. In order to stay on schedule, student's should make every effort to complete the current module's workload prior to the end of that module's week.

Module #	Topic	Week Starting
1	Introduction to Digital Forensics	2/1/21
2	Acquiring Evidence	2/8/21
3	Filesystems	2/22/21
4	Open-Source Forensic Tools	3/1/21
5	Windows / Mac / Linux Forensics	3/8/21
6	Advanced Windows Forensics	3/15/21
7	Programming for Digital Forensics	3/22/21
8	Application & Database Forensics	3/29/21

9	Network Forensics	4/5/21
10	Volatile Memory Analysis	4/12/21
11	Malware Analysis	4/19/21
12	Threat Hunting & Incident Response	4/26/21
13	Intrusion Analysis	5/3/21
14	Timeline Analysis	5/10/21

IMPORTANT DATES

- January 28, 2021 - Spring 2021 semester begins
- February 2, 2021 - First class meeting
- February 8, 2021 - Technical Writing Assignment Assigned
- April 11, 2021 - Technical Writing Assignment Submission Due
- April 25, 2021 - Technical Writing Assignment Peer Reviews Due
- May 2, 2021 - Final day for quizzes & forensic assignments - **NO EXTENSIONS**

CODE OF CONDUCT

Integrity is an integral part of the field of Digital Forensics. As such, students are reminded to review the code of conduct as it will be strictly enforced. All quizzes, forensic assignments and programming assignments are to be completed individually, without assistance from another person. You may use whatever outside non-human resources you desire (books, class notes, recorded lectures, internet research etc.). (https://engineering.nyu.edu/campus-and-community/student-life/office-student-affairs/policies/student-code-conduct)

MOSES CENTER STATEMENT OF DISABILITY

If you are a student with a disability who is requesting accommodations, please contact New York University's Moses Center for Students with Disabilities (CSD) at 212-998-4980 or mosescsd@nyu.edu. You must be registered with CSD to receive accommodations. Information about the Moses Center can be found at www.nyu.edu/csd. The Moses Center is located at 726 Broadway on the 2nd floor.